



COMMITTEE ON ENERGY AND COMMERCE
HEALTH
ENERGY
OVERSIGHT AND INVESTIGATIONS

COMMITTEE ON RULES

COMMITTEE ON BUDGET

Congress of the United States
House of Representatives

2161 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-7772
(202) 225-2919 FAX

2000 SOUTH STEMMONS FREEWAY
SUITE 200
LAKE DALLAS, TX 75065
(940) 497-5031
(940) 497-5067 FAX

www.house.gov/burgess

May 11, 2021

President Joseph R. Biden
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Dear President Biden:

On May 7, 2021, the Colonial Pipeline Company suffered a cybersecurity attack that forced the company to suspend the operation of its pipeline network.¹ On May 10, the Federal Bureau of Investigation (FBI) announced this event was a ransomware attack executed by the Russian hacker group known as “Darkside”.² Throughout your administration you have repeatedly stated your support for a modern, robust infrastructure; it is imperative that you and your cabinet fully explain to the Congress and the American public how you plan to address this crisis and prevent similar attacks in the future.

The Colonial Pipeline is a critical component of our nation’s energy infrastructure. It carries over 100 million gallons of refined petrochemicals from Texas to the East Coast, representing roughly 45% of the region’s supplies of diesel, gasoline, and jet fuel.³ If its operations are not quickly restored, energy prices will spike nationwide.⁴ Such a price increase could potentially spoil any hope of a quick economic recovery. This attack represents a dire threat to many American’s way of life and is the latest example of our critical infrastructure’s vulnerability to cyber threats from state and non-state actors.

Prior to the pandemic, the United States had finally realized its decades-long goal of energy independence.⁵ Today, Americans are scrambling to fill up their vehicles before a potential spike in fuel prices as gas shortages are being reported.⁶ These circumstances could quickly create a situation reminiscent of the Arab Oil Embargo of 1973.⁷ At least three states have declared a state of emergency in response to this ransomware attack and subsequent pipeline shutdowns. This is in addition to the regional state of emergency declared by the Department of Transportation. The federal government must take steps to protect consumers from the effects of vulnerabilities in our critical infrastructure.

¹ <https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption>

² <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks>

³ <https://www.colpipe.com/about-us/faqs>

⁴ <https://gasprices.aaa.com/gas-prices-jump-six-cents-on-week-likely-to-climb-higher-with-major-pipeline-shutdown/>

⁵ <https://www.instituteforenergyresearch.org/fossil-fuels/gas-and-oil/the-united-states-was-energy-independent-in-2019-for-the-first-time-since-1957/>

⁶ <https://nypost.com/2021/05/11/southeast-coast-suffers-gas-shortage-amid-pipeline-shutdown/>

⁷ <https://history.state.gov/milestones/1969-1976/oil-embargo>

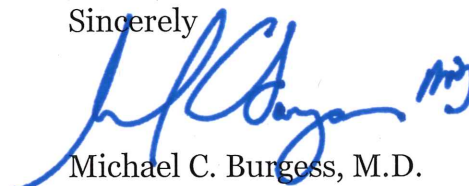
Reporting indicates that you will soon issue an executive order on federal cybersecurity, but it is unclear how this order would fit into a national cyber strategy to prevent similar attacks from occurring in the future on privately-owned critical infrastructure. The American people deserve to be confident in the security of their energy supplies.

To restore that confidence, we respectfully request comprehensive answers to the following questions:

1. Is the FBI confident this attack can be attributed to Darkside alone and that no adversarial nation-states were involved?
2. Is the federal government providing any resources to the Colonial Pipeline Company to ensure pipeline operations can resume as quickly as possible?
3. Will you commit to any action that ensures domestic supplies of refined petrochemical products can be delivered to consumers throughout the United States, including temporary waivers to the Jones Act and federal limits on the gross weight of fuel delivery vehicles?
4. How do you plan to bring the perpetrators of this attack to justice?
5. How is your administration coordinating with the many individuals and agencies with responsibility over cybersecurity to prepare for and prevent future attacks?
6. When you issue your executive order on federal cybersecurity, will this order clearly delineate the various lines of authority and jurisdiction between the various agencies that have responsibilities in cyber space?
7. Does your administration have a comprehensive national cyber strategy? If so, how would this strategy apply to the private sector?

Americans deserve reliable access to affordable, domestic energy products. This attack is only the latest threat to our nation's security, economic recovery, and energy independence. Our nation's energy infrastructure needs to be modernized and made more resilient to all threats natural and man-made, especially in the cyber domain. We look forward to your prompt attention to the above questions.

Sincerely



Michael C. Burgess, M.D.
Member of Congress

CC: The Honorable Jennifer M. Granholm, Secretary of Energy
CC: The Honorable Alejandro Mayorkas, Secretary of Homeland Security
CC: The Honorable Pete Buttigieg, Secretary of Transportation
CC: The Honorable Gina Raimondo, Secretary of Commerce
CC: The Honorable David P. Pekoske, Administrator of the Transportation Security Administration
CC: The Honorable Richard Glick, Chairman of the Federal Regulatory Commission
CC: The Honorable Chris Wray, Director of the Federal Bureau of Investigation
CC: The Honorable Michael S. Regan, Administrator of the Environmental Protection Agency

MB:my